4 設定例

この章では、以下の構成例に対し、本装置の設定方法を図と共に示します。

- 例1：単一サーバ構成
- 例2：複数サーバ構成
- 例3：複数の本装置をカスケード接続する構成
- 例4：送信用ルータと受信用ルータが異なる構成

表記上の規則

本書では、コマンドライン・インタプリタで用いるコマンドの説明において、以下の規則に従って表記を行います。

記号/字体	説明
< >	ユーザーが入力するパラメータを意味します。
[ ]	ユーザーが選択するパラメータを意味します。パラメータはそれぞれ「¦」で区切って表示されます。
{ }	省略可能なコマンドや省略可能なパラメータを意味します。
太字(ボールド体)	コマンドライン・インターフェースに対しユーザーが入力する実際の文字列を示します。コマンド実行の結果表示される文字列は通常の字体で表記されます。
¦	[ ]内の入力パラメータの区切りです。この記号で区切られている複数のパラメータのうち1つを選択します。実際の入力ではこの記号を入力しないでください。

例1：単一サーバ構成

この例では、本装置を単一のサーバと共に使用する場合の一般的な設定について述べます。ここでは自動マッピングを用いる場合と、手動設定(手動マッピング)を用いる場合の両方について述べます。この例は、本装置を使用する場合の最も簡単な例となります。

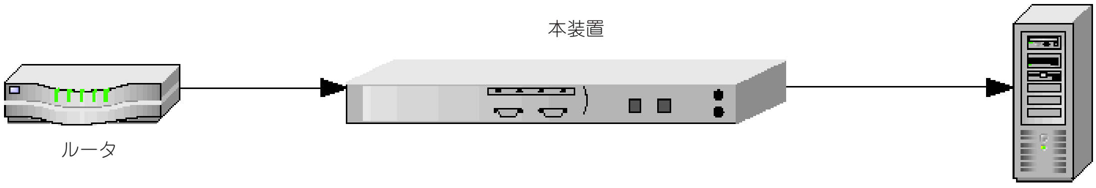


図4-1　単一サーバ構成

例1での手順

自動マッピング

1. 本装置をルータとサーバに物理的に接続します。
2. サーバへのHTTPSトラフィックを発生させます。本装置は、トラフィックを監視して、初期マッピング(および対応するデフォルトの鍵と電子証明書)を使用してHTTPSトラフィックを復号化し、クリア・テキストHTTPトラフィックをサーバに渡します。

手動設定

1. 第2章の手順に従って本体を設置します。次に、コマンドライン・インターフェースにアクセスしプロンプトを表示させてください。
2. 第3章の「鍵と電子証明書」で説明されている手順に従って、適切な鍵と電子証明書の設定を行ってください。
3. サーバに対するマッピングを作成します。create mapコマンドを用いて、サーバのIPアドレスとポート番号、そしてキーIDを関連づけます。

```
Intel 7110>create map
Server IP (0.0.0.0): 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

4. デフォルトのマッピングを削除します。マッピングを手動で作成した後に、デフォルトのマッピングを削除します。この例の場合はマップID番号1のマッピング(デフォルトのマッピング)を削除します。デフォルトのマッピングを削除するとマップID番号2のマッピングのマップID番号は1に変更されます。

```
Intel 7110>delete map 1
Intel 7110>list maps

Map                Net Ser Cipher Re-   Client
ID KeyID  Server IP Port Port Suites direct Auth

== =====  ========= ==== ==== ======  =====  ====

1  myserver 10.1.1.30 443 80 med(v2+v3) n   n
Intel 7110>
```

5. サーバのマッピングが作成されたら、その設定を保存します。

```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

例2：複数サーバ構成

この例では複数サーバ環境で設定する方法について説明します。

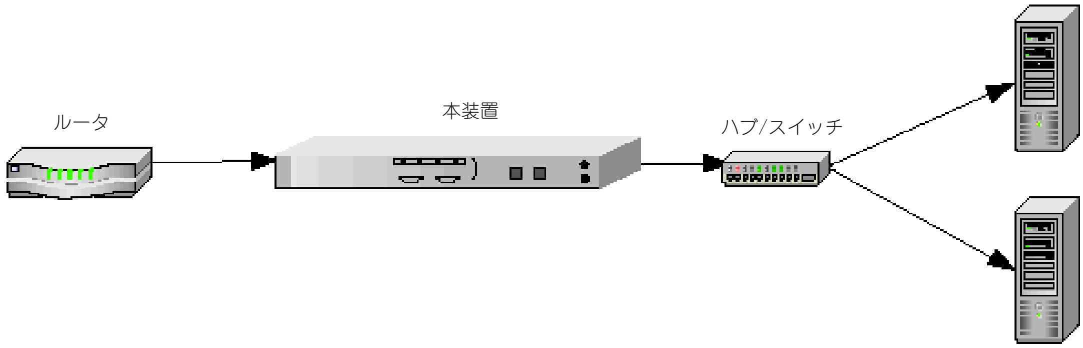


図4-2　複数サーバ構成

例2での手順

1. 第2章の手順に従って本体を設置します。次に、コマンドライン・インターフェースにアクセスしプロンプトを表示させます。
2. 第3章「鍵と電子証明書」で説明されている手順に従って適切な鍵と電子証明書を設定します。
3. サーバ1に対するマッピングを作成します。create mapコマンドを用いて、サーバのIPアドレスとポート番号、そしてキー IDを関連づけます。

```
Intel 7110>create map
Server IP: 10.1.1.30
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

4. サーバ2に対するマッピングを作成します。create mapコマンドを用いて、サーバのIPアドレスとポート番号、そしてキーIDを関連づけます。

```
Intel 7110>create map
Server IP: 10.1.1.31
SSL (network) port [443]: <Enter>
Cleartext (server) port [80]: <Enter>
KeyID to use for mapping: myserver
```

5. サーバが3台以上ある場合は、サーバ3以降のサーバに対して、上記の手順4の処理をIPアドレスをサーバのIPアドレスに変更して行います。

6. list mapsコマンドを使用して、現在の作成されているマッピングを表示します(複数の鍵と電子証明書をインポートし、それぞれのサーバに対してマップすることが可能です。この場合、それぞれの電子証明書内のフィールドの最低でも1つ(通常共有名)が、固有のものである必要があります。また、その時にはマップされるキー IDがそれぞれ異なっている必要があります)。

```
Intel 7110> list map

Map                 Net Ser Cipher Re-   Client
ID KeyID  Server IP Port Port Suites direct Auth

== =====  ========= ==== ==== ======  =====  ====

1 default  Any       443 80   all(v2+v3) n   n
2 myserver 10.1.1.30 443 80   med(v2+v3) n   n
3 myserver 10.1.1.31 443 80   med(v2+v3) n   n
Intel 7110>
```

7. デフォルトのマッピングを削除します。マッピングを手動で作成した後に、デフォルトのマッピングを削除します。この例の場合はマップID番号1のマッピング(デフォルトのマッピング)を削除します。デフォルトのマッピングを削除するとマップID番号2のマッピングのマップID番号は1に変更されます。

```
Intel 7110>delete map 1
Intel 7110>list map

Map                 Net Ser Cipher Re-   Client
ID KeyID  Server IP Port Port Suites direct Auth

== =====  ========= ==== ==== ======  =====  ====

1 myserver 10.1.1.30 443 80   med(v2+v3) n   n
2 myserver 10.1.1.31 443 80   med(v2+v3) n   n
Intel 7110>
```

8. サーバのマッピングが作成されたら、その設定を保存します。

```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

例3： 複数の装置をカスケード接続する構成

この例では複数の本装置をカスケードに接続し、その処理能力と可用性を拡張する場合の設定方法を説明します。この例では例1の手動設定と同じ手順を踏み、初段の装置を設定した後、その設定をエクスポートし、次段の装置にインポートします。

仮　定

- 2台以上の本装置を同じネットワーク上に接続します。本装置をカスケード接続するためには前段(ネットワーク側)の装置のサーバ用ポートを次段の装置のネットワーク用ポートに接続します。この接続を最終段までくりかえし、最終段の装置のサーバ用ポートをサーバに接続します(より詳しい情報については第2章の「インストールと初期設定」を参照してください)。
- 初段の本装置はすべて設定済みであり、必要な鍵、電子証明書、およびマップが存在していなければなりません。この設定を初段の装置からエクスポートし、次段の装置にインポートします。後段の装置についても、順番にこの手順を繰り返します。
- 初段の本装置上で、set spill enableコマンドを使用してスピル処理を有効にします。これで、初段の装置が処理できなかったデータは、次段の装置が処理します。後段の装置についても、順番にスピル処理を有効にします(最終段の装置を除く)。サーバにあふれ出た処理を引き継がせたい場合は、同様に、最終段の装置で、set spill enableコマンドを実行します(最終段でset spill enableとするためには、あふれた処理がサーバで処理され、そのためサーバでのクリア処理能力が低下し、サイト全体のパフォーマンスが低下する場合があります。十分な評価の元でその設定は行ってください)。

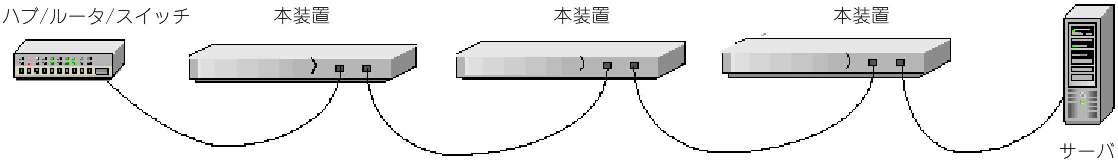


図4-3　複数の装置をカスケード接続する構成

例3での手順

1. サーバから一番離れた(初段の)装置に対し必要な設定(例えば例1の手動設定)を行います。後段に接続される他の装置はこの設定をエクスポートして使用します。
2. コマンドプロンプトからset spill enableと入力し、あふれ出た処理を後段に処理させるようにします。
3. 設定を保存します。

```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash

Intel 7110>
```

4. 設定をエクスポートします。export configコマンドを使用し、X modemモード(X)でエクスポートします。

```
Intel 7110> export config
Export protocol: (xmodem, uuencode, ascii)
[ascii]: x <Enter>
Beginning export...
```

5. ハイパーターミナルの転送メニューで受信を選択します。
6. ディレクトリ名を入力するか、または参照ボタンを使用して、受信したファイルを保存するディレクトリを指定します。
7. 受信プロトコルとしてxmodemを選択します。
8. 受信ボタンをクリックします。
9. 受信したファイルを保管するためのファイル名を指定し、OKをクリックします。処理は終了し、通常のプロンプトが再表示されます。

```
Use Ctrl-X to kill transmission
Export successful!
Intel 7110>
```

10. 2段目の本体にシリアルケーブルを接続し直し、パスワードを入力しコマンドプロンプトを表示させておきます。
11. 設定をインポートします。import configコマンドを用い処理を開始させます。まず、X modem(X)を選びます。そしてEnterキーを押し、本体内の実際のインポート処理を開始させます。

```
Intel 7110> import config
Import protocol: (paste, xmodem, uudecode)
[paste]: x <Enter>
Use Ctl-X to cancel upload
```

12. ハイパーターミナルの転送メニューで送信を選択します。
13. ファイル名を入力するか、または参照ボタンを使用して、送信するファイルを指定します。
14. 送信プロトコルとしてxmodemを選択します。
15. 送信ボタンをクリックします。転送が完了し、この設定をインストールするかどうか確認するプロンプトが表示されます。

```
Do you want to install this config ? [y]: y
```

16. 了承(y)すると、プロンプトが再表示されます。

```
Intel 7110>
```

17. 設定を保存します。

```
Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

18. 上記の手順11〜17を3段目以降に接続した装置に対して繰り返します。最終段の装置上で、set spill disableコマンドを使用してスピル処理を無効にします。そしてconfig saveで設定を保管します。

19. 必要に応じて、最終段の装置でset spill enableコマンドによって、あふれ出た処理のサーバに引き渡すように設定します。この設定を行った場合は、再度config saveコマンドで設定を保存してください。

例4：送信用ルータと受信用ルータが異なる構成

本装置に接続されたルータとして本装置側からの送信用ルータと受信ルータを異なったものを使用する場合の構成についての説明です。

仮　定

- 単一または複数のサーバを接続します。
- 1台以上の本装置を用います(複数の本装置をカスケードすることも可能です)。
- 1台以上の受信用ルータ(クライアント側からサーバ側へのトラフィックを扱うルータ)
- 1台の送信用ルータ(サーバ側からクライアント側へのトラフィックを扱うルータ)

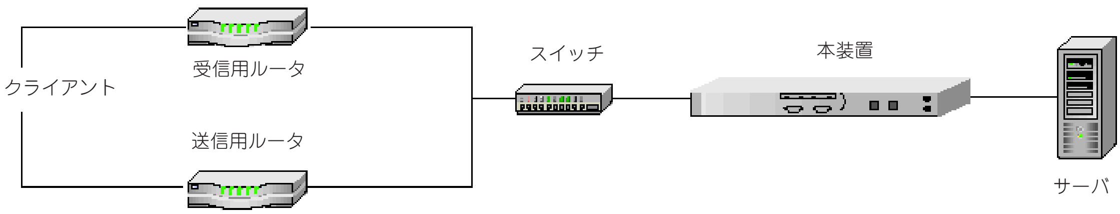


図4-4　送信用ルータと受信用ルータが異なる構成

例4での手順

1. 本装置の一般的な(送受信用のルータが同じ場合の)設定を行います(サイト構成に合わせて、例えば前述の例で行った設定を行います)。
2. 本装置からクライアント側へ送るトラフィックを扱う送信用ルータのMACアドレスを調べます。
3. コマンドラインから、デフォルトで用いる送信用ルータを指定し、設定を保存します。

```
Intel 7110>set egress_mac 00:11:22:33:44:55
Egress MAC set to 00:11:22:33:44:55

Intel 7110>config save
Saving configuration to flash...
Configuration saved to flash
Intel 7110>
```

> ヒント
>
> サーバのデフォルトゲートウェイとして、送信用ルータが設定されている場合は(この設定が必要な場合は、そのようになっているはず)、arp -aコマンドをサーバから実行してデフォルトゲートウェイのMACアドレスを得ることができます。このMACアドレスを使用してください。

4. 設定を無効にするためには以下のように入力します。

```
Intel 7110>set egress_mac none
```

~Memo~